


Administrative - Internal Use Only

IHSA-82-040

4 OCT 1982

MEMORANDUM FOR: Chief, Management Staff, ODP

FROM:


Information Handling Systems Architect

STAT

SUBJECT: Comments on Proposed FIPS, "Standard on Computer Data Integrity"

1. Our perusal of this FIPS does not reveal the purpose for its creation. It would appear to be the "bright idea" of an ICST staffer, who then wrote a standard to "sell it". We are unaware of any existing application of a public key system for this purpose for which standardization is required. The primary and first defense of data is DES encryption, which the ICST has already standardized. We are unaware why anybody would want to add 'a character-for-character' check of message integrity when the message is already encrypted. If the DES encryption does not safeguard the integrity of the message, then the addition of a DES integrity check certainly will not. One-for-one integrity checking is also unacceptably inefficient for most conceivable applications.

2. Lacking any background information which would justify the creation of this standard, it is the opinion of this office that it should not be issued. This standard appears to be a misuse of the standards process. Hopefully, it is not a portent of a new direction. Standards should be written to standardize the interfaces and data formalisms that system developers and equipment manufacturers already are using. They should not be used as a medium to sell new concepts or dictate new applications.

STAT

memo from MS, etc in FIPS folder

Administrative - Internal Use Only